PART II.

NATIONAL AND INTERNATIONAL CYBERSECURITY ASPECTS

CASE STUDIES

CYBER SECURITY

STRATEGIES FOR COUNTERING CYBER THREATS

LEGAL NORMS FOR CYBER SPACE

Canada Research Centre

A due process of Cyber Security Definitions

There are no common definitions for Cyber terms. [CCDCOE]

'Cybersecurity is the ability to protect or defend the use of cyberspace from cyber attacks.' [CCDCOE]

Cybersecurity can be discussed on different levels the most engaging being the operational seen as "the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. [NIST, US DoC]

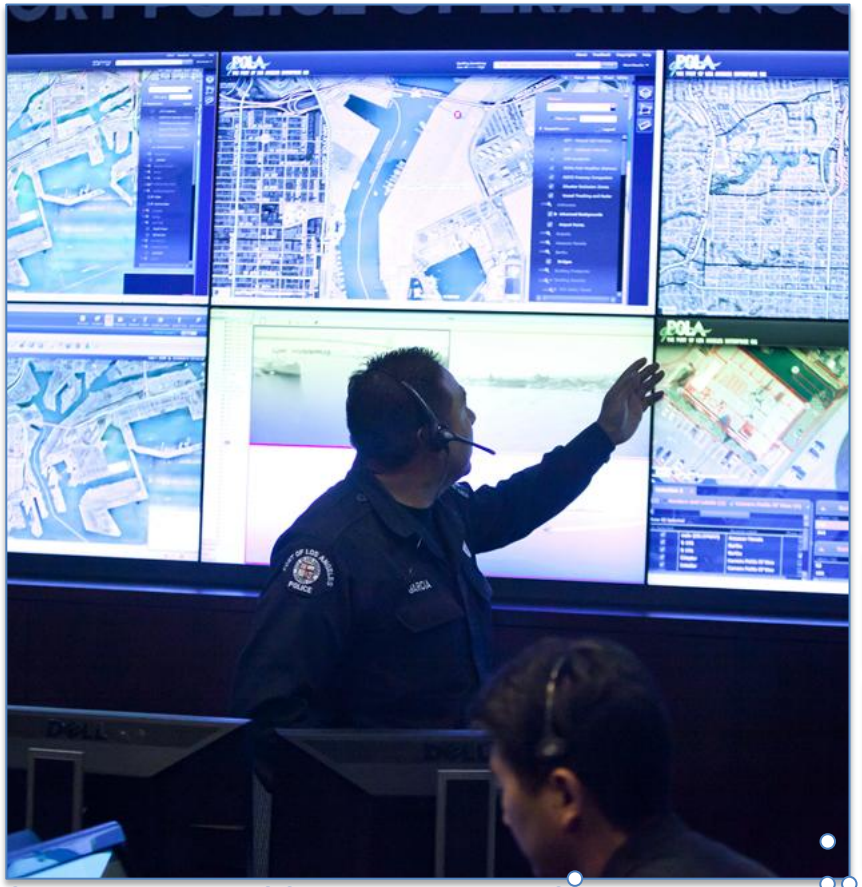
National & International Cyber Security Aspects

Canada Research Centre

WebHoppe- an experimental mapping of Internet traffic in real-time developed by Sensorium.

The Fog of War in Cyber Space

Canada Research Centre



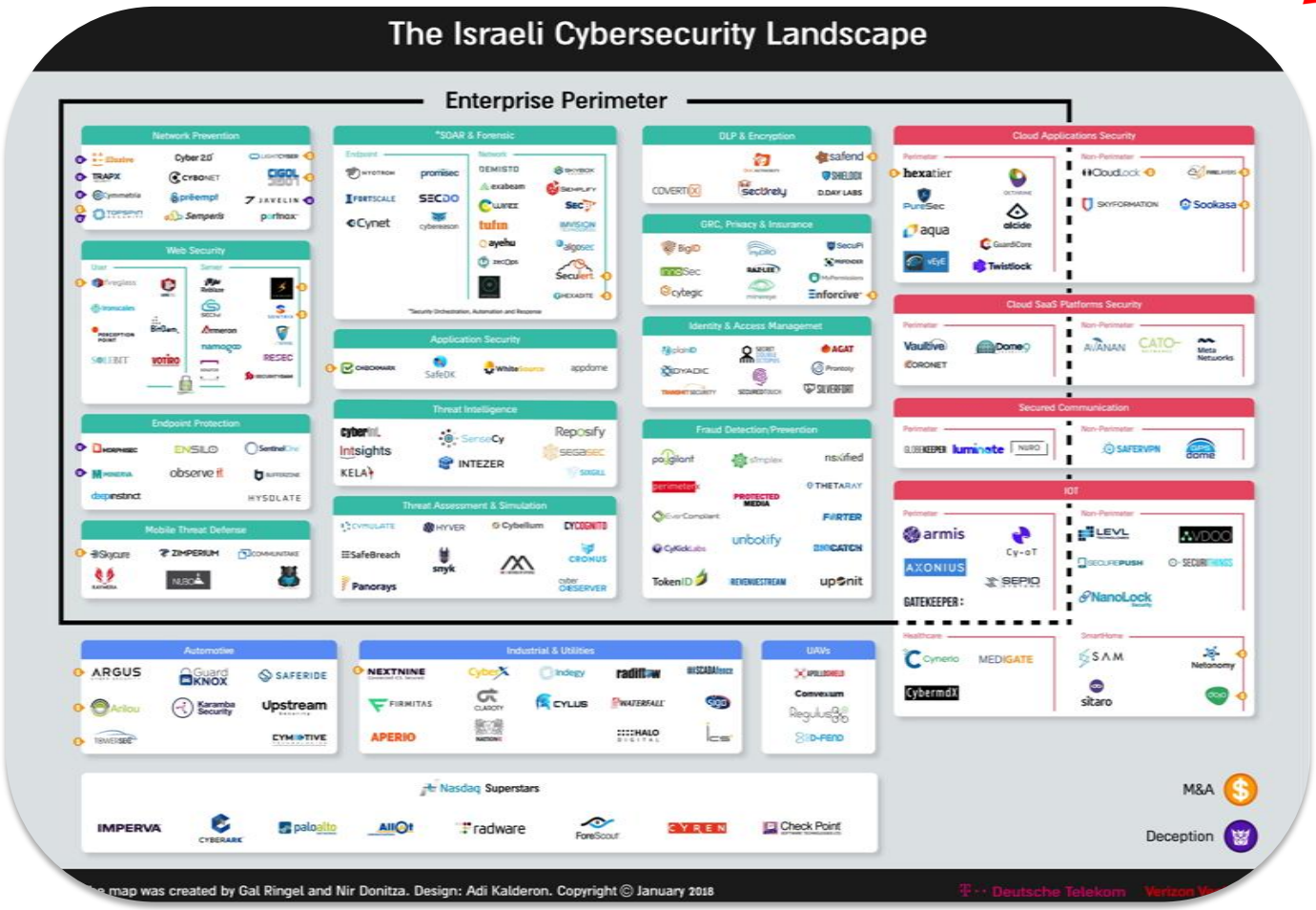
Adversaries' aggression and coercion work just below the level that would risk military confrontation with the West.

Canada Research Centre

National Cyber Security Strategies	**China's National Cyberspace Security Strategy has cyber threats, competition among major powers, militarization of cyberspace, and cyberspace governance and rules-making in focus**
	US National Defense Strategy-return to great power rivalry [Russia & China] – building a more lethal force to compete strategically while including the cyber space. Cyberspace national strategy yet to be announced.

The US Congress' sets priorities in the cyber space for the White House/DOD, e.g. establish national standards and guidance in the cybersecurity and cyber-warfare space; establish national standards and guidance in the cybersecurity and cyber-warfare space; the national incident response plan; plans to defend, mitigate, and interrupt attacks on infrastructure critical to the political integrity, economic security; enhancing the cyber resilience ; offensive cyber capabilities; strengthening attributions and cyber threat intelligence to effectively detect, disrupt and expose malicious cyber activities.

Canada Research Centre



This info-graphic map shows 199 out of over 500 Israeli companies specializing only in preventive/defensive Cyber Security measures.

Image: Verizon ventures

Canada Research Centre

Inter-national aspect of Cyber Security

Cybersecurity is an international problem that requires an international solution.

The necessary progress on international cyber security will most likely come from within the European Union and NATO.

The international law is applicable to cyberspace.

Cyber defence is part of NATO's core task of collective defence, i.e. **Article V.**

NATO has affirmed that **international law** applies in cyberspace, including the UN Charter, international humanitarian law, and human rights law as applicable.

The main focus in cyber defence is to **protect** its own networks and **enhance resilience** across the Alliance.

Allies also made a **'Cyber Defence Pledge'** [2016] to enhance their cyber defences, as a matter of priority.

Resilient national cyber defences are vital to the collective defence.

The NATO Industry Cyber Partnership to maintaining an edge in military technology over its adversaries through agile acquisition, early engagement and closer partnership with industry, private sector and academia.

Malware Information Sharing Platform. Note: Joining instructions and Terms-of-Use can be obtained by sending an email request to MISPsupport@ncirc.nato.int

The security of the Alliance and its ability to conduct agreed tasks of collective defence, crisis management and cooperative security is, to a large extent, dependent upon the cyber-defence capability and capacity of its individual Allies.

The new **NATO Cyber Operations Center** will facilitate NATO's a proportional responses to cyber attacks, by either conventional or cyber means which could elicit an Article 5-level response

Supporting conceptual bases for cyber defense **NATO accredited national Centers of Excellence**, i.e.Cooperative Cyberdefense Center of Excellence, Tallinn, Riga, Strategic Communications Center of Excellence, Latvia, Riga, European Center of Excellence for Countering Hybrid Threats, Finland, Helsinki.

The most substantial and necessary progress on international cyber domain and its security aspects will primarily be developed within the EU. It raises cyber security standards including **capacity building for civilian cyber security, support for training, increased cooperation between law enforcement** to tackle cybercrime and policy making.

The **Directive on Security of Network and Information Systems** (the NIS Directive); Impending deadline for its transposition into national legislation [by May 9, 2018] & **Identification of operators of essential services** [by November 9, 2018]. *It provides legal measures to boost the overall level of Cybersecurity in the EU.*

The **"NIS toolkit"**: Commission adopted [2017] a Communication that aims at supporting Member States in their efforts to implement the Directive swiftly and coherently across the EU.

The EU cyber security strategy [2013] and **the EU cyber defence policy framework** [2014] as part of the Common Security and Defence Policy (CSDP) are the basis for NATO-EU cooperation in cyber domain.

A frame work for a joint NATO-EU **diplomatic response against coercive cyber operations** is being discussed.

The European Defence Agency (EDA), on the other hand, plays a role in ensuring operational synergies between the EU and NATO.

Cyber Attacks Case studies

The proverbial Pandora's box is opened, the capability of cyber tools have been demonstrated. And that raises the worrisome questions!?

How effective any weapons will prove in the event if an opponent is able to degrade their capabilities?

How effective will any fighting forces be when the communication links fail, when commanders have to make decisions on their own, and when GPS no longer provides accurate readings or any readings at all?

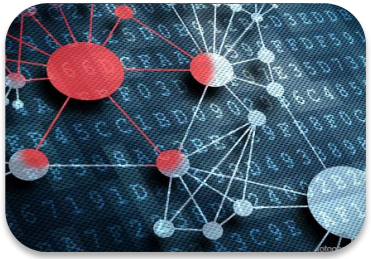
How can any industry be protected against cyber attacks while attackers are using the same technology and following the same tech-revolution in cyber capabilities?

Infamouss Cyber Attacks

Canada Research Centre

Black Swan[s]

The Impact of the Highly Improbable



"Web War One" in Estonia

Cyber attack 'STUXNET'

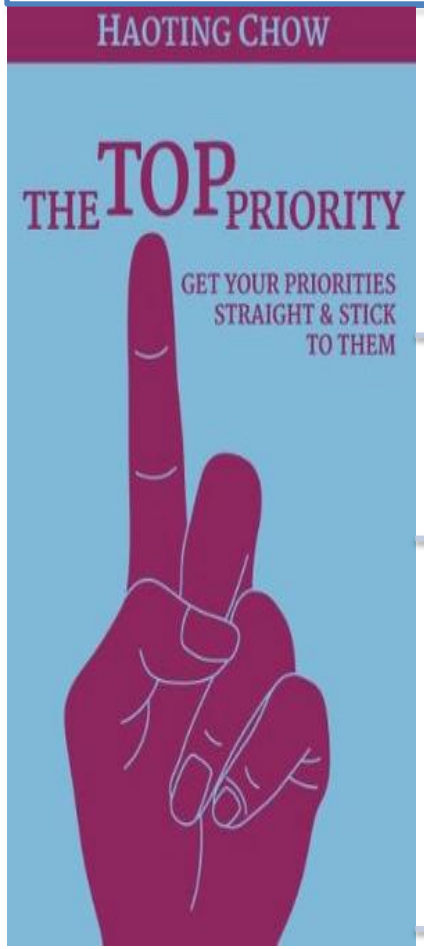
The case of EQUIFAX

Cyber Attack "NotPetya'

The case of UBER

The case of Deloitte.

Countering Cyber Threats



Regulatory frameworks, protective measures and protocols - a common aspiration of states, industries and technology providers – defined through dialogue.

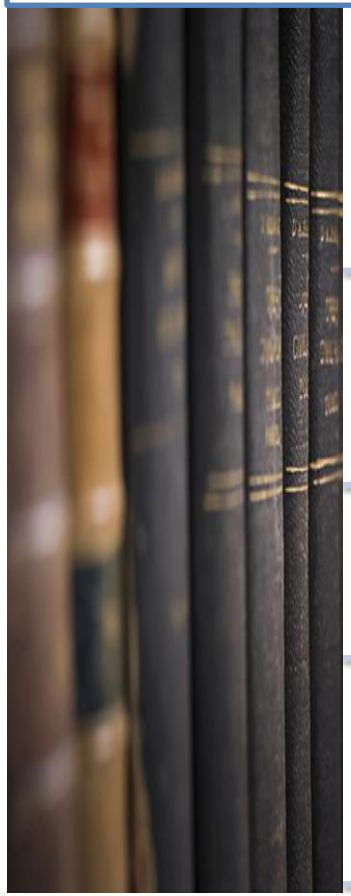
Public-private partnerships to mitigating cyber threats.

Building a collective defense & resilience at international [NATO, the EU, the OSCE], national [Whole of Government Approach], & at societal level, across industries, and private sector, individually…

We share the responsibility!

Legal and Regulatory Framework in Cyber Space

Canada Research Centre



Calls for norms to secure and stabilize cyberspace have become pervasive.

Political sensibilities over norms in Cyber Space.

Lack of shared understanding.

Attribution, escalation and proportionality conundrum.

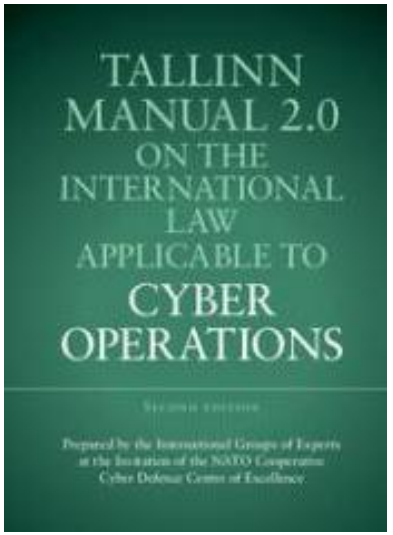
Constitutional, Legislative, Regulatory Bodies

Canada Research Centre

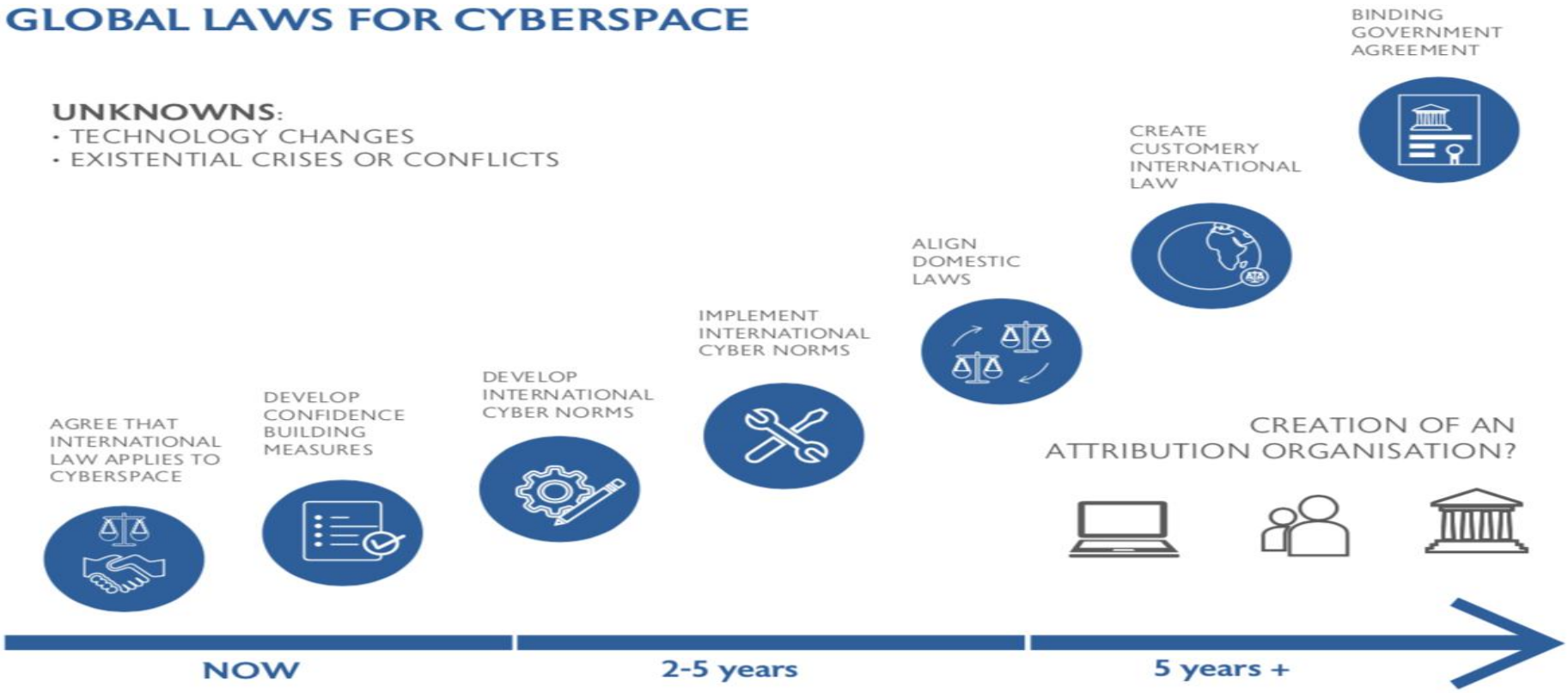
UN/SC

EU

States



Canada Research Centre



Source WEF athttps://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention

The United Nations

After thirteen years of the UN çyberwarfare talks the 'UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security' (GGE) came to a stole in 2017 over the right to self-defence in the face of attacks and the question of attribution for a foreign cyber-attack.

2012/2013 UN GGE providing that 'international law is applicable to cyberspace including the UN charter itself'. Reafirmed by Permanent Five [US, UK, France, China, Russia].

2016/2017 UN GGE tasked to set an international legal framework to "help reduce the risk of conflict by creating stable expectations of how states may and may not respond to cyber incidents they face." No agreement was reached…

The European Union

Global General Data Protection Regulation [GDPR], in force on May 2018; Law applies to all companies with operations in the EU collecting and processing data belonging to EU citizens.

EU's Directive on security of network and information systems [NIS Directive] as regulatory instrument directing member countries to be equipped and prepared to respond to incidents through a Computer Security Incident Response Team [CSIRT]; In force on May 9, 2018.

"NIS toolkit" – a manual for NIS Directive implementation.

The Convention on Cybercrime of the Council of Europe (2001), known as the Budapest Convention, is the only binding international instrument on this issue.

Other binding agreements

Bilateral cyber security agreements [the Sino-Russian, US-China, US-India, Sino-Anglo, China-Australia cyber security agreements…

G-7 expressed the support for cyber security norms. **G-20** affirmed in a statement that no country should "conduct or support cyber-enabled theft of intellectual property"

Regional international organizations have similarly acknowledged the applicability of international law to cyberspace, including the ASEAN Regional Forum and the Organization of American States.

National defence policies gradually resource efforts in building defensive and offensive capabilities to disrupt that of their adversaries.